PROOFS

Proofs

- Proof: a valid argument that establishes the truth of a statement.
- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent

Theorem

- Theorem: a statement that can be shown to be true using:
  - definitions
  - other theorems
  - axioms (statements which are given as true)
  - rules of inference
- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.
- For example, the statement: "If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$" really means "For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$."

Proving Theorem

- Many theorems have the form: $\forall x\,(P(x) \rightarrow Q(x))$
- To prove them, we show that where *c* is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$

Proving Conditional Statements

- **Trivial Proof**

  If we know q is true, then $p \rightarrow q$ is true as well.

  Example: "If it is raining, then 1=1."

- **Vacuous Proof**

  If we know p is false then $p \rightarrow q$ is true as well.

  Example: "If I am both rich and poor, then $2 + 2 = 5$."

Proving Conditional Statements: Direct Proof

- **Direct Proof**

Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

Example 1:

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Assume that n is odd. Then $n = 2k + 1$ for an integer k.

Squaring both sides of the equation, we get: $n^2 = (2k + 1)^2$

$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1$, where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then n^2 is an odd integer.

Example 2:

Prove that the sum of two rational numbers is rational.

Assume r and s are two rational numbers. Then there must be integers p, q and also t, u such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \; q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu} = \frac{v}{w}$$

where $v = pu + qt$
$w = qu \neq 0$

Thus the sum is rational.

Proving Conditional Statements: Indirect Proof

- **Proof by Contraposition**

Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an indirect proof method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.

Example 1:

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Assume n is even. So, $n = 2k$ for some integer k.

Thus $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$.

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even).

Example 2:

Prove that for an integer n, if n^2 is odd, then n is odd.

Use proof by contraposition. Assume n is even (i.e., not odd).

Therefore, there exists an integer k such that $n = 2k$.

Hence, $n^2 = 4k^2 = 2(2k^2)$ and n^2 is even (not odd).

We have shown that if n is an even integer, then n^2 is even.

Therefore by contraposition, for an integer n, if n^2 is odd, then n is odd.

▪ **Proof by Contradiction**

To prove p, assume $\neg p$ and derive a contradiction such as

$p \wedge \neg p$ (an indirect form of proof). Since we have shown that

$\neg p \rightarrow F$ is true , it follows that the contrapositive $T \rightarrow p$ also holds.

Example 1:

Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Assume that no more than 3 of the 22 days fall on the same day of the week. Because there are 7 days of the week, we could only have picked 21 days. This contradicts the assumption that we have picked 22 days.

Example 2:

Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors.

Then $$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (an exercise). Since a is even, $a = 2c$ for some integer c.

Thus, $$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore b^2 is even. Again then b must be even as well.

But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational.

Contradiction vs Contrapositive Methods

- Advantage of contradiction method:
  - Contrapositive method only for universal conditional statements.
  - Contradiction method is more general.
- Advantage of contrapositive method:
  - Easier structure: after the first step, Contrapositive method requires a direct proof.
  - Contradiction method normally has more complicated structure.

- **Proof by Counterexample**

Recall $\exists x \neg P(x) \equiv \neg \forall x\, P(x)$.

To establish that $\neg \forall x\, P(x)$ is true (or $\neg \forall x\, P(x)$ is false) find a c such that $\neg P(c)$ is true or $P(c)$ is false.

In this case c is called a counterexample to the assertion.

Example 1:

"Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

Proving Biconditional Statements

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Example:

Prove the theorem: "If n is an integer, then n is odd if and only if n^2 is odd." We have already shown that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$. Sometimes iff is used as an abbreviation for "if an only if," as in "If n is an integer, then n is odd iff n^2 is odd."

Proof Strategies for Proving $p \rightarrow q$

- Choose a method
  - First try a direct method of proof.
  - If this does not work, try an indirect method (e.g., try to prove the contrapositive).
- For whichever method you are trying, choose a strategy
  - First try forward reasoning. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q, or start with $\neg q$ and prove $\neg p$.
  - If this doesn't work, try backward reasoning. When trying to prove q, find a statement p that we can prove with the property $p \rightarrow q$.

Mathematical Induction

Mathematical induction is a legitimate method of proof for all positive integers n.

Principle:

Let P_n be a statement involving n, a positive integer. If

1. P_1 is true, and
2. the truth of P_k implies the truth of P_{k+1} for every positive k,

then P_n must be true for all positive integers n.

Example:

Find P_{k+1} for $P_k : S_k = \dfrac{3(2k+1)}{k-1}$.

$$P_{k+1} : S_{k+1} = \frac{3[2(k+1)+1]}{k+1-1}$$ Replace k by $k + 1$.

$$= \frac{3(2k+2+1)}{k}$$ Simplify.

$$= \frac{3(2k+3)}{k}$$ Simplify.

Example:

Use mathematical induction to prove

$$S_n = 2 + 4 + 6 + 8 + \cdots + 2n = n(n + 1)$$

for every positive integer n.

1. Show that the formula is true when $n = 1$.

$$S_1 = n(n + 1) = 1(1 + 1) = 2 \qquad \text{True}$$

2. Assume the formula is valid for some integer k. Use this assumption to prove the formula is valid for the next integer, $k + 1$ and show that the formula $S_{k+1} = (k + 1)(k + 2)$ is true.

$$S_k = 2 + 4 + 6 + 8 + \cdots + 2k = k(k + 1) \qquad \text{Assumption}$$

Example continued:

$$S_{k+1} = 2 + 4 + 6 + 8 + \cdots + 2k + [2(k + 1)]$$

$$= 2 + 4 + 6 + 8 + \cdots + 2k + (2k + 2)$$

$$= S_k + (2k + 2)$$ Group terms to form S_k.

$$= k(k + 1) + (2k + 2)$$ Replace S_k by $k(k + 1)$.

$$= k^2 + k + 2k + 2$$ Simplify.

$$= k^2 + 3k + 2$$

$$= (k + 1)(k + 2)$$

$$= (k + 1)((k + 1)+1)$$

The formula $S_n = n(n + 1)$ is valid for all positive integer values of n.

Sums of Powers of Integers :

1. $$\sum_{i=1}^{n} i = 1+2+3+4+\cdots+n = \frac{n(n+1)}{2}$$

2. $$\sum_{i=1}^{n} i^2 = 1^2+2^2+3^2+4^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

3. $$\sum_{i=1}^{n} i^3 = 1^3+2^3+3^3+4^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$$

4. $$\sum_{i=1}^{n} i^4 = 1^4+2^4+3^4+4^4+\cdots+n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

5. $$\sum_{i=1}^{n} i^5 = 1^5+2^5+3^5+4^5+\cdots+n^5 = \frac{n^2(n+1)^2(2n^2+2n-1)}{12}$$

Example:

Use mathematical induction to prove for all positive integers *n*,

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$S_1 = \frac{1(1+1)(2(1)+1)}{6} = \frac{1(2)(2+1)}{6} = \frac{6}{6} = 1$$ True

$$S_k = 1^2 + 2^2 + 3^2 + 4^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$ Assumption

$$S_{k+1} = 1^2 + 2^2 + 3^2 + 4^2 + \cdots + k^2 + (k+1)^2$$

$$= S_k + (k+1)^2$$

$$= S_k + k^2 + 2k + 1$$ Group terms to form S_k.

$$= \frac{k(k+1)(2k+1)}{6} + k^2 + 2k + 1$$ Replace S_k by $k(k+1)$.

Example continued:

$$= \frac{2k^3 + 3k^2 + k}{6} + \frac{6k^2 + 12k + 6}{6}$$

Simplify.

$$= \frac{2k^3 + 9k^2 + 13k + 6}{6}$$

$$= \frac{(k^2 + 3k + 2)(2k + 3)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$$= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

The formula $S_n = \frac{n(n+1)(2n+1)}{6}$ is valid for all positive integer values of *n*.